

JC821 U.S. PRO
09/905195
07/16/01

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日

Date of Application:

2000年 7月18日

出願番号

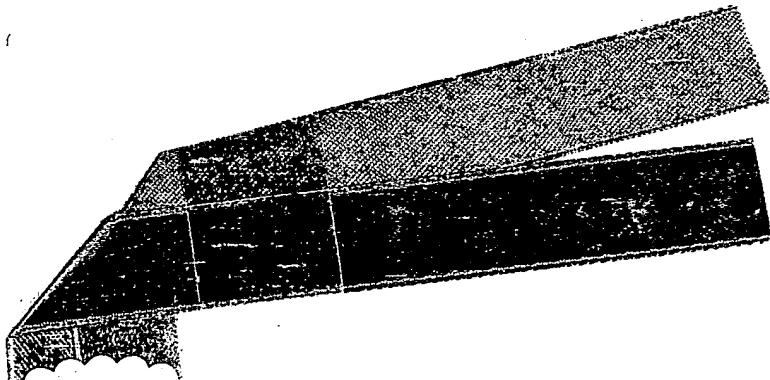
Application Number:

特願2000-216983

出願人

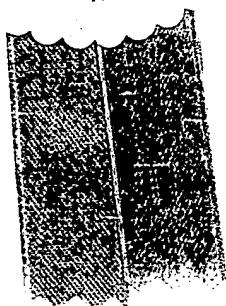
Applicant(s):

株式会社 沖マイクロデザイン
沖電気工業株式会社



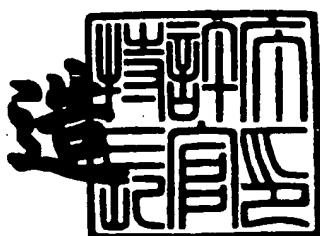
CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月 9日



特許庁長官
Commissioner,
Patent Office

及川耕



出証番号 出証特2001-3006941

【書類名】 特許願
【整理番号】 SI003835
【提出日】 平成12年 7月18日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 12/14
【発明者】
【住所又は居所】 宮崎県宮崎郡清武町大字木原 7083番地 株式会社
沖マイクロデザイン内
【氏名】 新森 信明
【特許出願人】
【識別番号】 591049893
【氏名又は名称】 株式会社 沖マイクロデザイン
【特許出願人】
【識別番号】 000000295
【氏名又は名称】 沖電気工業株式会社
【代理人】
【識別番号】 100089635
【弁理士】
【氏名又は名称】 清水 守
【選任した代理人】
【識別番号】 100096426
【弁理士】
【氏名又は名称】 川合 誠
【選任した代理人】
【識別番号】 100116307
【弁理士】
【氏名又は名称】 青木 俊明
【手数料の表示】
【予納台帳番号】 012128

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001052

【包括委任状番号】 9001053

【包括委任状番号】 0008808

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体回路

【特許請求の範囲】

【請求項1】 JTAGポートとTAPの間にフラッシュROMのセキュリティビットで制御されるJTAG制御回路を具備することを特徴とする半導体回路。

【請求項2】 フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン汎用ポートをPinスクランブル回路にてデコードする回路を設け、前記Pinスクランブル回路の出力の逆相を前記インヒビットNANDゲートの片方に入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする半導体回路。

【請求項3】 フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン内部レジスタとしてデバッグインターブルレジスタを設け、前記インヒビットNANDゲートに前記デバッグインターブルレジスタの出力の逆相を入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする半導体回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、半導体回路に関するものである。

【0002】

【従来の技術】

図4はかかる従来の半導体回路としてのJTAG回路の構成図である。

【0003】

この図において、1はJTAG (Joint Test Action Group) ポート、2, 4はTAP (Test Access Port)、3はCPUコア、5はフラッシュ (Flash) ROMである。

【0004】

昨今のマイコン（マイクロコントローラ）では、JTAG等を使用したデバッグ機能が搭載されているマイコンが主流になってきている。このデバッグ機能を使用してマイコンのソフト開発者はアプリケーションソフトのデバッグを行い、容易にプログラムを開発できるようになっている。

【0005】

また、最近多くなっているフラッシュROM内蔵マイコンでは、JTAGを使用してフラッシュROMの書換えが実行できるようになっている。そして、このフラッシュROMにはセキュリティビットを設け、フラッシュROMの内容が第三者に読み出せないようになっている。因みに、フラッシュROMに書き込まれるデータは、ユーザー作成のアプリケーションプログラムであり、上記したセキュリティビットをセットすると、フラッシュROMのライタでの読み出し及び部分的な領域の書換えが不可能になる（例えば、特開平11-85620号公報参照）。

【0006】

【発明が解決しようとする課題】

しかしながら、上記した従来のフラッシュROMのセキュリティはセキュリティビットに“1”をセット後はJTAGを使用したフラッシュROMライタではフラッシュROMの内容が読み出されないようにになっているが、JTAGを使用したデバッグ機能では、図4に示すように、JTAGインターフェースとしてのJTAGポート1のTAP2にてCPUコア3に対し直接命令を挿入できるため、フラッシュROM5の内容を容易にダウンロードできる。このためセキュリティビットの意味をなしていない。

【0007】

本発明は、上記問題点を除去し、フラッシュROMの内容が第三者に読み出されることを防止することができる半導体回路を提供することを目的とする。

【0008】

【課題を解決するための手段】

本発明は、上記目的を達成するために、

- [1] 半導体回路において、JTAGポートとTAPの間にフラッシュROM

のセキュリティビットで制御されるJTAG制御回路を具備することを特徴とする。

【0009】

[2] 半導体回路において、フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン汎用ポートをPinスクリンブル回路にてデコードする回路を設け、前記Pinスクリンブル回路の出力の逆相を前記インヒビットNANDゲートの片方に入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする。

【0010】

[3] 半導体回路において、フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン内部レジスタとしてデバッグイネーブルレジスタを設け、前記インヒビットNANDゲートに前記デバッグイネーブルレジスタの出力の逆相を入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする。

【0011】

【発明の実施の形態】

以下、本発明の実施の形態について詳細に説明する。

【0012】

まず、本発明の第1実施について説明する。

【0013】

図1は本発明の第1実施例を示す半導体回路の回路図である。

【0014】

この実施例では、JTAGポート1とTAP2, 4の間に、信号を禁止したり許可したりすることのできるJTAG制御回路6を設け、この制御をフラッシュROM5のセキュリティビットで行うように構成したものである。なお、図1において、3はCPU(中央処理装置)である。

【0015】

以下、この実施例の回路の動作について説明する。

【0016】

プログラマーはJTAGポート1を使用してデバッグを行いプログラムの開発を行うが、プログラムの開発が終了すると、フラッシュROM5のセキュリティビット(SEQ)に“1”を書込む。セキュリティビットが“1”になるとJTAG制御回路6に禁止信号として入力され、JTAGポート1とTAP2, 4間の信号のやり取りが禁止され、結果としてJTAGポート1を使用したデバッグが使用できなくなる。つまり、JTAGポート1とTAP2, 4の間にORゲート(論理を変えればANDゲートでも可能)を挿入し、SEQ=1となったら、TAP2, 4には“1”しか入力されなくなるような回路構成にする。

【0017】

このように第1実施例によれば、フラッシュROM5のセキュリティビットに“1”を書込むとJTAGポート1を使用したフラッシュROMライタによる読み出しだけでなく、JTAGポート1を使用したデバッグ機能も使用不可能となるため、フラッシュROM5の内容が第三者に読み出されることが全く無くなる。

【0018】

次に、本発明の第2実施例について説明する。

【0019】

図2は本発明の第2実施例を示す半導体回路の回路図である。なお、第1実施例と同じ部分には同じ符号を付してその説明は省略する。

【0020】

この実施例ではフラッシュROM5とJTAG制御回路6のJTAG制御ポートとの間にインヒビット(INHIBIT)NANDゲート7を設け、且つマイコンの汎用ポート9をデコードするPinスクランブル回路8を設けるようにしたものである。なお、Pinスクランブル回路8は汎用ポート9のうち1本または数本をデコードし、インヒビットNANDゲート7に入力するもので、チップ毎にマスクオプション等で指定できるものである。

【0021】

以下、この実施例の回路の動作について説明する。

【0022】

上記した第1実施例と同様にプログラマーはデバッグ終了後にフラッシュROM5のセキュリティビットに“1”を書き込み、第三者がJTAGポート1を使用したデバッグ機能によるフラッシュROM5の内容の読み出しを禁止する。しかし、セキュリティ書き込み後でもチップ毎に設定されたPinスクランブル回路8で汎用ポート9をデコードすることにより、JTAGポート1でのデバッグが可能となる。

【0023】

このように第2実施例によれば、フラッシュROM5のセキュリティビット書き込み後もチップ毎に設定されたPinスクランブル回路8の内容（マスクオプション等の内容）を知っているプログラマーはJTAGポート1を使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Pinスクランブル回路8を知らない第三者にはJTAGポート1を使用したデバッグは使用できないため、フラッシュROM5の内容が第三者に漏れることはない。

【0024】

次に、本発明の第3実施例について説明する。

【0025】

図3は本発明の第3実施例を示す半導体回路の回路図である。なお、第1実施例と同じ部分には、同じ符号を付してそれらの説明は省略する。

【0026】

この実施例ではフラッシュROM5のセキュリティビットとJTAG制御回路6との間のインヒビットNANDゲート7の一つに入力されるデバッゲイネーブル(DBG_EN)レジスタ10というマイコンの内部レジスタを設けるようにしたものである。

【0027】

以下、この実施例の回路の動作について説明する。

【0028】

上記した第1及び第2実施例と同様に、プログラマーはデバッグ終了後はフラッシュROM5のセキュリティビットに“1”を書き込み、第三者によるフラッシ

ュROM5の内容の読み出しを禁止する。しかし、プログラムの一部にレジスタに“1”をセットするプログラムを用意しておき、必要に応じてそのプログラムを起動し、デバッグイネーブルレジスタ10を“1”にセットすることにより、JTAGポート1でのデバッグが可能となる。

【0029】

このように第3実施例によれば、第2実施例と同様に、フラッシュROM5のセキュリティビット書き込み後もデバッグイネーブルレジスタ10のセットのプログラムを起動することにより、JTAGポート1でのデバッグが可能となる。また、第2実施例と異なりプログラム的に制御するのでマスクオプション等の無駄な費用が発生しない。更に、当然デバッグイネーブルレジスタ10のセットのプログラムの起動はフラッシュROM5のプログラムの内容を理解しているプログラム開発者のみが実行できるもので、プログラムの内容を知らない第三者がデバッグイネーブルレジスタ10をセットすることはできない。

【0030】

したがって、フラッシュROM5のセキュリティビット書き込み後のデバッグが容易に行え、且つ第三者がフラッシュROM5の内容をJTAGポート1でのデバッグ機能を使用して読み出すことを防止することができる。

【0031】

なお、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づいて種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0032】

【発明の効果】

以上、詳細に説明したように、本発明によれば、次のような効果を奏すことができる。

(1) フラッシュROMのセキュリティビットに“1”を書き込むとJTAGポートを使用したフラッシュROMライタによる読み出しだけでなく、JTAGポートを使用したデバッグ機能も使用不可能となるため、フラッシュROMの内容が第三者に読み出されることが全く無くなる。

(2) フラッシュROMのセキュリティビット書き込み後もチップ毎に設定された

Pinスクランブル回路の内容（マスクオプション等の内容）を知っているプログラマーはJTAGポートを使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Pinスクランブルを知らない第三者にはJTAGポートを使用したデバッグは使用できないためフラッシュROMの内容が第三者に漏れることはない。

(3) 上記(2)と同様にフラッシュROMのセキュリティビット書き込み後もデバッグイネーブルレジスタのセットのプログラムを起動することにより、JTAGポートでのデバッグが可能となる。また、上記(2)と異なりプログラム的に制御するものでマスクオプション等の無駄な費用が発生しない。また、当然デバッグイネーブルレジスタのセットのプログラムの起動はフラッシュROMのプログラムの内容を理解しているプログラム開発者のみが実行できるものでプログラムの内容を知らない第三者がデバッグイネーブルレジスタをセットすることはできない。したがって、フラッシュROMのセキュリティビット書き込み後のデバッグが容易に行え、且つ第三者がフラッシュROMの内容をJTAGポートでのデバッグ機能を使用して読み出すことを防止することができる。

【図面の簡単な説明】

【図1】

本発明の第1実施例を示す半導体回路の回路図である。

【図2】

本発明の第2実施例を示す半導体回路の回路図である。

【図3】

本発明の第3実施例を示す半導体回路の回路図である。

【図4】

従来の半導体回路としてのJTAG回路の構成図である。

【符号の説明】

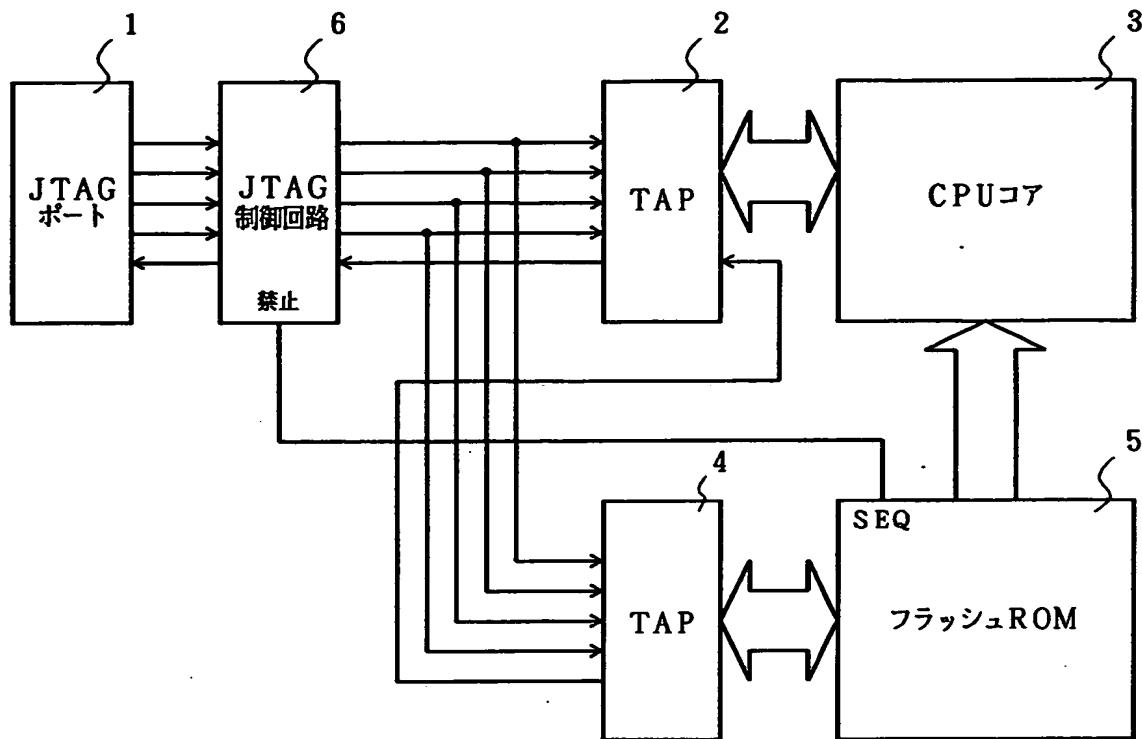
- 1 JTAGポート
- 2, 4 TAP
- 3 CPUコア
- 5 フラッシュROM

- 6 J T A G 制御回路
- 7 インヒビット (INHIBIT) NANDゲート
- 8 Pinスクランブル回路
- 9 マイコンの汎用ポート
- 10 デバッグイネーブル (DBG_EN) レジスタ

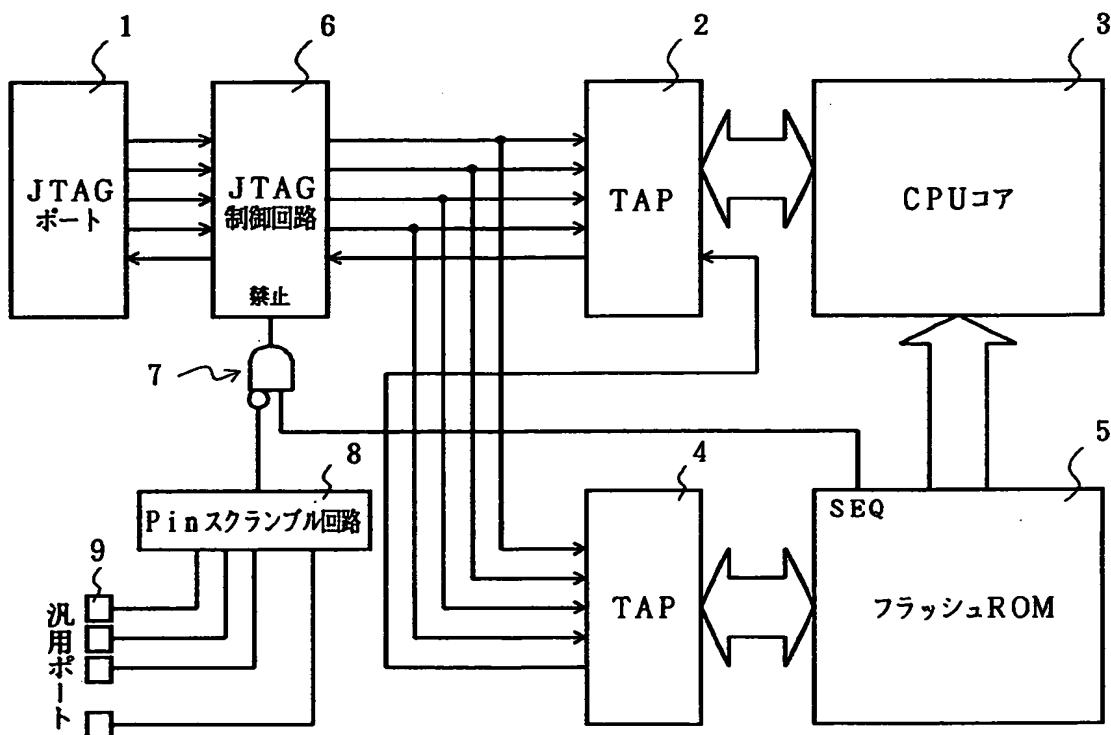
【書類名】

図面

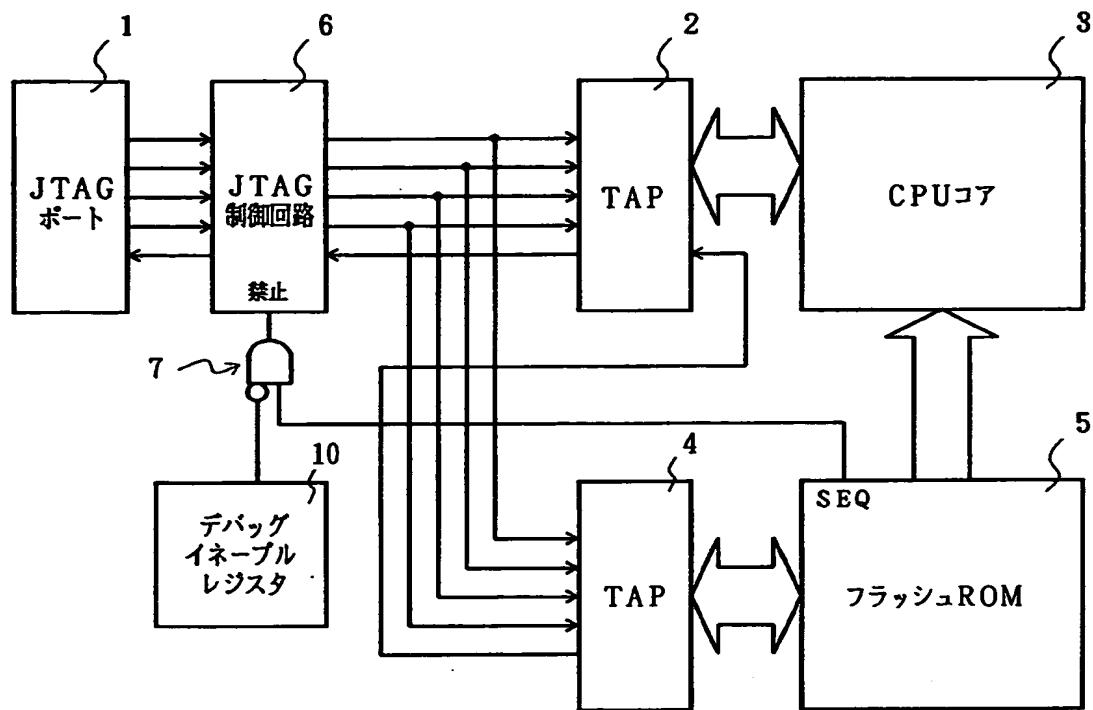
【図1】



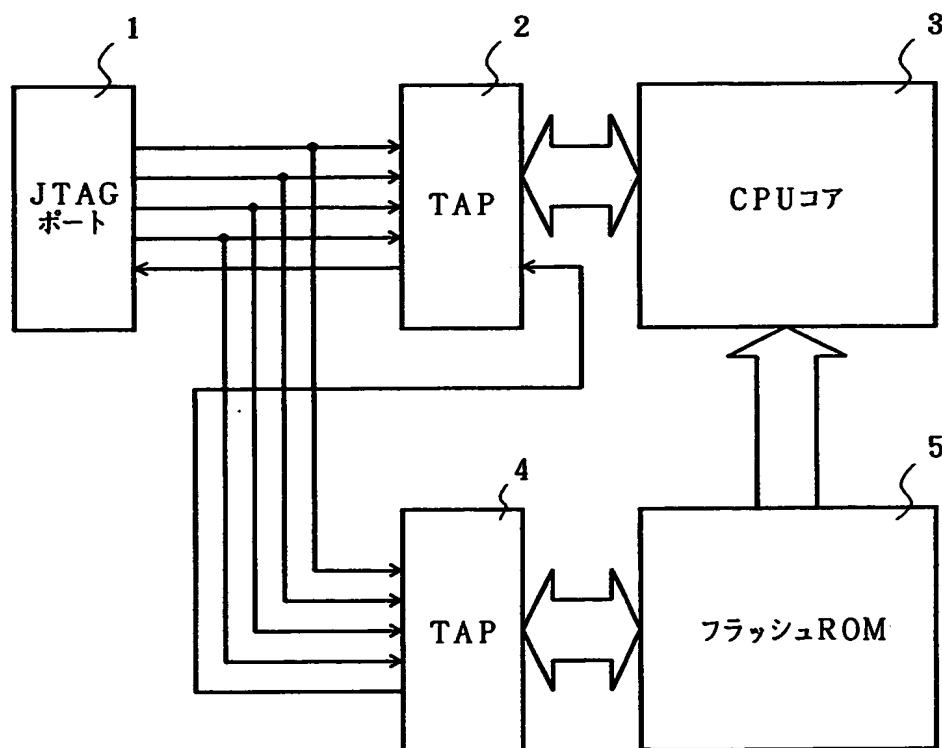
【図2】



【図3】



【図4】



【書類名】 要約書

【要約】

【課題】 フラッシュROMの内容が第三者に読み出されることを防止することができる半導体回路を提供する。

【解決手段】 半導体回路において、フラッシュROM5のセキュリティビットに“1”を書き込むと、JTAGポート1を使用したフラッシュROMライタによる読み出しだけでなく、JTAGポート1を使用したデバッグ機能も使用不可能となるため、フラッシュROM5の内容が第三者に読み出されることが全く無くなる。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-216983
受付番号	50000905695
書類名	特許願
担当官	濱谷 よし子 1614
作成日	平成12年 7月27日

<認定情報・付加情報>

【特許出願人】

【識別番号】	591049893
【住所又は居所】	宮崎県宮崎郡清武町大字木原7083番地
【氏名又は名称】	株式会社 沖マイクロデザイン

【特許出願人】

【識別番号】	000000295
【住所又は居所】	東京都港区虎ノ門1丁目7番12号
【氏名又は名称】	沖電気工業株式会社

【代理人】

【識別番号】	100089635
【住所又は居所】	東京都千代田区神田美土代町7番地10 大園ビル
【氏名又は名称】	清水 守

【選任した代理人】

【識別番号】	100096426
【住所又は居所】	東京都千代田区神田美土代町7番地10 大園ビル
【氏名又は名称】	川合 誠

次頁無

出願人履歴情報

識別番号 [591049893]

1. 変更年月日 1999年 6月17日

[変更理由] 名称変更

住 所 宮崎県宮崎郡清武町大字木原7083番地

氏 名 株式会社 沖マイクロデザイン

出願人履歴情報

識別番号 [000000295]

1. 変更年月日 1990年 8月22日

[変更理由] 新規登録

住 所 東京都港区虎ノ門1丁目7番12号

氏 名 沖電気工業株式会社